

REMARKS

The Examiner has rejected Claims 1-18 under 35 U.S.C. 102(b) as being anticipated by Walsh et al. (U.S. Patent No. 5,956,481). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove.

In particular, it appears that the Examiner has not taken into consideration the full weight of applicant's claims. For example, the Examiner relies on the following excerpt from Walsh to make a prior art showing of applicant's claimed "assigning an identifier to the process if no identifier is assigned thereto."

"For yet another aspect of the present invention, each session of the program module can be assigned a digital session key." (col. 6, lines 18-20)

Such excerpt, however, fails to meet applicant's claimed conditional limitation. In particular, Walsh teaches assigning a digital session key for "each session." In sharp contrast, applicant teaches and claims "assigning an identifier to the process if no identifier is assigned thereto" (emphasis added).

Moreover, the Examiner relies on the following excerpt from Walsh to make a prior art showing of applicant's claimed "identifying a process for accessing files and selecting virus detection actions based at least in part on the identified process."

"Turning now to FIG. 2, which is a logical flow diagram generally describing the steps of a virus protection routine 200, an open file event is detected in step 202. The open file event initiates the opening of a file or document for processing by a program module, such as a word processing program. In response to detecting the opening of a file, an inquiry is conducted at step 204 to determine whether the file contains a known virus component. For example, if the virus-

in-issue is a macro virus, such as the "Concept" virus, the file to be opened can be examined to determine whether it includes a macro or a customization. If a determination is made that the file to be opened is unlikely to contain the virus, the "NO" branch is followed from step 204 to step 206. In step 206, the file is opened by completing a conventional open operation associated with the file open event. On the other hand, if the file includes characteristics associated with a virus, the "YES" branch is followed from step 204 to step 208." (col. 10, lines 17-34)

This excerpt, however, merely identifies an "open file event," not the "process for accessing files." Moreover, since Walsh fails to identify the process itself, it fails to disclose, teach or suggest "Selecting virus detection actions based at least in part on the identified process" (emphasis added). Only applicant teaches and claims the identification of the process itself that is accessing files for the purpose of tailoring the virus detection actions based on the process, in the manner claimed.

To further emphasize this point of differentiation, applicant now specifies the aforementioned process in greater detail by claiming "the process ...[being] associated with an application program, and different identifiers ...[being] assigned to different application programs so that the virus detection actions are tailored for the processes associated with the application programs."

Walsh merely suggests that "each session of the program module can be assigned a digital session key" so that "[i]n response to detecting another open file event for this selected file, a comparison can be made between the digital signature saved with the selected file and the digital session key for the present session" and responding based on the comparison. Instead of randomly assigning keys to each session, like that taught in Walsh, applicant teaches and claims assigning "different identifiers ... to different application programs." By uniquely identifying the application programs in such a manner, applicant is capable of tailoring virus detection actions for the processes associated with the application programs, in the manner claimed. Simply nowhere in the prior art is there such a combination of

features for application program-specific identifiers and associated virus detection actions.

The Examiner's proposed rejection is further deficient with respect to many of the dependent claims. Specifically, the Examiner relies on the following excerpt from Walsh to make a prior art showing of applicant's claimed "identifier ...[being] cleared upon the occurrence of a predetermined event," and "the event ...[being] the termination of an application." See Claims 2-3, 8-9, and 14-15.

"In response to detecting another open file event for this selected file, a comparison can be made between the digital signature saved with the selected file and the digital session key for the present session." (col. 6, lines 22-26)

Such excerpt (and the remaining Walsh reference), however, fails to make any mention of clearing an identifier upon the termination of an application.

Still yet, the Examiner relies on the following excerpt from Walsh to make a prior art showing of applicant's claimed "the identifier ...[being] assigned by the application," and "the application ...[being] adapted for executing the process." See Claims 5-6, 11-12, and 17-18.

"For yet another aspect of the present invention, each session of the program module can be assigned a digital session key." (col. 6, lines 18-20)

However, such excerpt, along with the remaining Walsh reference, simply fails to disclose, teach or suggest that the application (that is adapted to execute the process) assigns the identifier.

Applicant has even further amended the claims to emphasize still additional features, as follows:

"wherein the virus detection actions are selected by determining a category associated with the process based on the identifier, and selecting a set of virus detection actions based on the determined category" (see Claim 19)

"wherein the identifier reflects a risk level associated with the application program, and a plurality of categories each have virus detection actions tailored for an associated risk level" (see Claim 20)

A notice of allowance or a specific showing in the prior art of such features is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P003/00.069.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100

NAI1P003/00.069.01

- 9 -